(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 26 326 A 1**

(51) Int. Cl.[7]:
H 04 Q 7/34
H 04 L 9/32
H 04 M 1/66

(21) Aktenzeichen: 100 26 326.7
(22) Anmeldetag: 26. 5. 2000
(43) Offenlegungstag: 29. 11. 2001

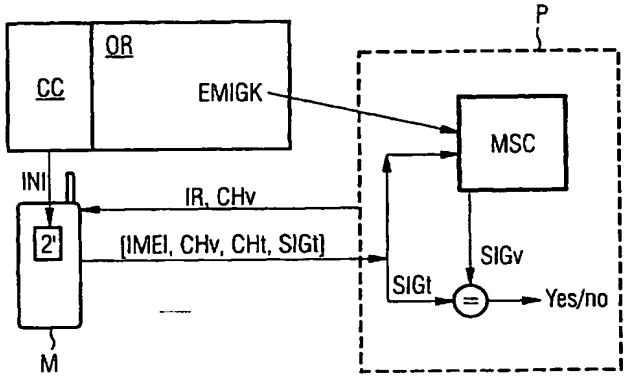
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Adi, Wael, Dr.-Ing., 38108 Braunschweig, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur kryptografisch prüfbaren Identifikation einer physikalischen Einheit in einem offenen drahtlosen Telekommunikationsnetzwerk

(57) Die Erfindung schafft ein Verfahren zur Identifikation einer physikalischen Einheit (M) in einem offenen, drahtlosen Telekommunikationsnetzwerk durch eine Prüfeinrichtung (P) mit den Schritten: Speichern einer geheimen Identität (SIMEI) und einer offenen Identität (IMEI) in der physikalischen Einheit (M); Erzeugen eines ersten Parameters (CHv) in der Prüfeinrichtung (P); Senden einer Identifikationsaufforderung (IR) mit dem ersten Parameter (CHv) von der Prüfeinrichtung (P) an die physikalische Einheit (M); Erzeugen einer elektronischen Unterschrift (SIGt) durch eine erste Krypto-Funktion (F3) aus der geheimen Identität (SIMEI) und mindestens dem ersten Parameter (CHv) in der physikalischen Einheit (M) und Senden der erzeugten elektronischen Unterschrift (SIGt) und der offenen Identität (IMEI) an die Prüfeinrichtung (P); Erzeugen der geheimen Identität (SIMEI) aus einem offenen Schlüssel (EMIGK) und der gesendeten offenen Identität (IMEI) in der Prüfeinrichtung (P); Erzeugen einer entsprechenden elektronischen Unterschrift (SIGv) durch die erste Krypto-Funktion (F3) aus der erzeugten ersten geheimen Identität (SIMEI) und mindestens dem ersten Parameter (CHv) in der Prüfeinrichtung (P); und Identifizieren der physikalischen Einheit (M) durch einen Vergleich der gesendeten elektronischen Unterschrift (SIGt) und der erzeugten entsprechenden elektronischen Unterschrift (SIGv) in der Prüfeinrichtung (P).



DE 100 26 326 A 1

DE 100 26 326 A 1

Beschreibung

STAND DER TECHNIK

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur kryptografisch prüfbaren Identifikation einer physikalischen Einheit in einem offenen, drahtlosen Telekommunikationsnetzwerk.

[0002] Obwohl auf beliebige Telekommunikationseinrichtungen anwendbar, werden die vorliegende Erfindung, sowie die ihr zugrundeliegende Problematik in Bezug auf Mobilfunksysteme erläutert.

[0003] GSM-Mobilfunksysteme und diese betreffende kryptographische Verfahren sind z. B. in Asha Mehrotra, "GSM System Engineering", Artech Haus Pub., 1996, oder in D. R. Stinson, "Cryptography Theory and Practice", CRC Press, 1995, beschrieben.

[0004] Die Identität eines mobilen Terminals bzw. (End)geräts wird allgemein als IMEI (International Mobile Equipment Identity) bezeichnet. Sie definiert ein einziges Gerät individuell und liefert dafür eine komplette eindeutige Spezifikation.

[0005] **Fig. 7** ist eine schematische Darstellung eines bekannten Identifikationsmechanismus eines Mobiltelefons gegenüber einem Netzwerkbetreiber.

[0006] In **Fig. 7** bezeichnet M ein Mobiltelefon mit einer zentralen Verarbeitungseinheit 1 und einem Identitätsmodul 2, welcher einen zugriffssicheren Bereich TA aufweist, in dem die Identität IMEI gespeichert ist.

[0007] Die momentane Erkennung eines solchen Gerätes M (Mobile Equipment) basiert heute im GSM-System darauf, dass das Gerät M sich durch seine IMEI offen vorstellt. Es wird gefordert, daß die Gerätehersteller dafür sorgen sollen, daß IMEI im Gerät M nicht modifizierbar ist, und daß die Software des Gerätes M immer nach Aufforderung des Netzes nur die richtige, im Gerät gespeicherte IMEI liefert.

[0008] Der Einsatz im gestrichelten Rahmen von **Fig. 1** zeigt eine Darstellung für die allgemeine Implementierung dieses Identifikationsmechanismus. Nach einer Identitätsanfrage ("Identity request") IR liefert das Gerät M den Parameter IMEI, der vom Hersteller IO in eine geschützte Speicherzelle eingeprägt worden ist, als Reaktion an den Netzwerkbetreiber.

[0009] Dieses Verfahren ist leicht zu fälschen. Ein Softwaresprung J im Software-Identifikationssystem SS kann (wie in **Fig. 1** zu sehen) jede andere Identifikation IMEI' anstelle der korrekten Identifikation IMEI liefern. Dies ist immer dann möglich, wenn man die Software des Gerätes M ändern kann, was üblicherweise leicht ist, oder wenn man die Identität IMEI ändern kann, was in der Regel etwas schwieriger ist. Das größte Problem dabei ist aber, dass geklonte Geräte nach Belieben eine Identität IMEI liefern können. Dabei braucht man nur einmal das Netz abzuhören und eine legale IMEI in Erfahrung zu bringen, da IMEI stets offen gesendet wird. Man kann aber auch legitime IMEI-Identifikationen selber generieren, da die Einstellung bekannt ist. Somit bietet diese Art der Identifikation keinen besonderen Sicherheitsstandard.

[0010] **Fig. 8** ist eine schematische Darstellung eines weiteren bekannten Identifikationsmechanismus eines Mobiltelefons gegenüber einem Netzwerkbetreiber nach der Challenge & Response-Technik.

[0011] Gesicherte Identifikation durch die sogenannte Challenge & Response-Technik ist in Kryptosystemen eine bekannte Technik, um die Identität eines Geräts festzustellen.

[0012] Die Technik baut, wie in **Fig. 8** dargestellt, auf die Frage und Antwort auf. Die Prüfstation (z. B. eine Basisstation des Netzwerkbetreibers) P sendet an das geprüfte Gerät M eine Identifikationsanfrage AR mit einer in einem Zufallsgenerator RG erzeugten Zufalls-Symbolfolge RAND "challenge pattern" aus 128 Bits und fordert von ihm eine bestimmte Reaktion ARE "Response" mit einem Datenwort SRES aus 32 Bits, das nachweist, daß das geprüfte Gerät M einen bestimmten Geheimwert K_i mit 128 ebenso wie die Prüfstation P Bits besitzt, welcher zusammen mit RAND durch eine Abbildung A3 zu einem Prüfergebnis SRES verknüpfbar ist, das vom geprüften Gerät M an die Prüfstation P retourniert wird.

[0013] Die Abbildung A3 ist eine stark nicht lineare Abbildung, die sehr schwer umkehrbar ist (oft als Einweg Funktion bezeichnet), wie in Asha Mehrotra aaO. dargestellt. Die Abbildung A3 wird in der Regel als ein Block-Chiffrierverfahren ausgewählt. Die beiden, Prüfer P und Geprüfter M, erhalten den gleichen Response SRES, falls die beiden geheimen Schlüssel K_i beim Prüfer P und beim Geprüften M identisch sind. In diesem Fall ist das Identifizierungsresultat ARES positiv, ansonsten negativ.

[0014] Dieser Vorgang kann mehrmals mit unterschiedlichen Zufallswerten RAND wiederholt werden, um die Sicherheit zu erhöhen. Diese Verfahren wird schon im GSM-System eingesetzt, aber nur um einen Benutzer durch seine Benutzerkarte USIM zu identifizieren. Durch zunehmende Bedrohung durch Cloning (Nachbau) und Diebstahl von Mobilfunkgeräten ist die Notwendigkeit gestiegen, einen Mechanismus im Mobilgerät zu integrieren, der das Gerät veranlasst, sich selbst zu identifizieren, und somit gestohlene sowie geklonte oder nicht zertifizierte Geräte in einem Netz zu erkennen. Dies erfordert aber die Kenntnis des Parameters K_i durch Prüfer und Geprüften. Da es aber in einem drahtlosen Netz viele Service-Anbieter und viele Hersteller gibt, sind komplexe Verwaltung und Austausch aller K_i's im Netz zwischen Hersteller und Netzbetreiber notwendig.

[0015] Die Anzahl der zu identifizierenden Einheiten sowie deren Hersteller ist in heutigen Kommunikationsnetzen groß und ändert sich laufend. Dies erhöht den Verwaltungs- und Wartungsaufwand weiter.

VORTEILE DER ERFINDUNG

[0016] Das erfindungsgemäße Verfahren mit den Merkmalen des Anspruchs 1 bzw. die entsprechende Vorrichtung nach Anspruch 7 weisen gegenüber dem bekannten Lösungsansatz den Vorteil auf, dass ein auf der C & R-Technik basierender Identifikationsmechanismus geschaffen wird, der keine hohen Verwaltungs- und Wartungsaufwand erfordert. Die Erfindung ermöglicht die Identifikation einer Netzeinheit durch eine möglichst einfache im Netz vorhandene Hardwareinfrastruktur mit möglichst einfacher Verwaltung und möglichst wenig Kommunikation.

[0017] Die der vorliegenden Erfindung zugrundeliegende Idee besteht darin, daß nach einer modifizierten Challenge Response Technik überprüft wird, ob eine physikalische Einheit eine bestimmte geheime Identität enthält, ohne diese Identität zu lesen, und auch ohne diese Identität vorher zu kennen. Damit wird die Echtheit der Identität der physikaischen Einheit bzw. des Gerätes bewiesen. Das erfindungsgemäße Verfahren beruht auf einer Geheim-Kryptographie-Technik in Verbindung mit einer Anordnung von bestimmten Hardware Einheiten und mit einem Protokoll.

[0018] Das erfindungsgemäße Verfahren basiert auf der Speicherung von einer einzigartigen geheimen Identität in einem geschützten Register innerhalb des zu identifizierenden Geräts und eines geheimen Herstellerschlüssels innerhalb einer Vorrichtung, z. B. einer Smartcard, beim Prüfenden. Die geheime Identität bzw. der geheime Hersteller-

schlüssel wird durch eine Hardware-Einrichtung nicht lesbar gemacht, wie z. B. in Asha Mehrotra, "GSM System Engineering", Artech Haus Pub., 1996, offenbart. Das Gerät ist aber in der Lage, von sich Information zu geben, die die einzigartige Identität des Gerätes durch die Technik von Challenge & Response (C & R) nachweist.

[0019] Die Technik der Challenge & Response ist eine an sich bekannte Technik und findet verbreitete Anwendung in kryptographisch gesicherten Systemen zwecks Identifikation. Die besonderen Merkmale dieses Verfahrens sind:

- kein Register für die Identitäten der einzelnen Geräte wird benötigt;
- keine gemeinsame Kenntnis der geheimen Identität durch Prüfer und Geprüfter ist nötig;
- die Lösung ist angepasst an die Gegebenheiten und Umgebung von Mobiltelefonen mit vielen Dienstanbietern und Herstellern, die international arbeiten und schwachen Informationsaustausch und Koordinationsmöglichkeiten haben; und
- die Technik baut Einheiten auf, die schon im System vorhanden sind.

[0020] Die Erfindung ist eine Erweiterung der Challenge Response Technik, um die Identifikation weniger komplex und dadurch flexibel und kostengünstiger zu gestalten. Die neue Technik nutzt in einer bevorzugten Ausgestaltung Internet Server und moderne Smart-Card-Technik.

[0021] In den Unteransprüchen finden sich vorteilhafte Weiterbildungen und Verbesserungen des Gegenstandes der Erfindung.

[0022] Gemäß einer bevorzugten Weiterbildung wird der offene Schlüssel durch eine zweite Krypto-Funktion aus einem ersten geheimen Schlüssel und einem zweiten geheimen Schlüssel erzeugt.

[0023] Gemäß einer weiteren bevorzugten Weiterbildung wird die geheime Identität durch eine dritte Krypto-Funktion aus der offenen Identität und dem zweiten geheimen Schlüssel erzeugt.

[0024] Gemäß einer weiteren bevorzugten Weiterbildung wird in der Prüfeinrichtung der erste geheime Schlüssel gespeichert wird und die geheime Identität durch folgende Schritte in der Prüfeinrichtung erzeugt: Erzeugen des zweiten geheimen Schlüssels durch die Inverse zur zweiten Krypto-Funktion aus dem ersten geheimen Schlüssel und dem offenen Schlüssel; und Erzeugen der geheimen Identität durch die dritte Krypto-Funktion aus aus der offenen Identität und dem erzeugten zweiten geheimen Schlüssel.

[0025] Gemäß einer weiteren bevorzugten Weiterbildung wird der offene Schlüssel über das Internet an die Prüfeinrichtung gesendet.

[0026] Gemäß einer weiteren bevorzugten Weiterbildung erfolgen ein Erzeugen eines zweiten Parameters in der physikalischen Einheit; ein Senden des zweiten Parameters an die Prüfeinrichtung; und ein Erzeugen der elektronischen Unterschrift und der entsprechenden elektronischen Unterschrift aus der geheimen Identität und dem ersten und zweiten Parameter.

[0027] Gemäß einer weiteren bevorzugten Weiterbildung werden der erste und der zweite Parameter durch eine exklusive ODER-Funktion verknüpft.

[0028] Gemäß einer weiteren bevorzugten Weiterbildung werden der erste und der zweite Parameter multiplexiert und anschließend durch eine exklusive ODER-Funktion verknüpft, wobei es eine Rückkopplung vom Ausgang der ersten Krypto-Funktion zur exklusiven ODER-Funktion gibt. Eine derartige nicht-lineare Funktion erhöht die Sicherheit zusätzlich.

[0029] Gemäß einer weiteren bevorzugten Weiterbildung werden der erste und/oder zweite Parameter als Zufallsgrößen vorgesehen.

[0030] Gemäß einer weiteren bevorzugten Weiterbildung ist das Telekommunikationsnetzwerk ein Mobiltelefonsystem.

[0031] Gemäß einer weiteren bevorzugten Weiterbildung sind die erste, zweite und dritte Krypto-Funktion die gleiche Funktion.

[0032] Gemäß einer weiteren bevorzugten Weiterbildung ist die gleiche Funktion eine Standardfunktion.

[0033] Gemäß einer weiteren bevorzugten Weiterbildung werden die Schritte e) und f) auf einer Smard-Card in der Prüfeinrichtung durchgeführt.

ZEICHNUNGEN

[0034] Ausführungsbeispiele der Erfindung sind in den Zeichnungen dargestellt und in der nachfolgenden Beschreibung näher erläutert.

[0035] Es zeigen:

[0036] **Fig.** 1 eine schematische Darstellung der Teilnehmer und des Systemaufbaus bei einer ersten Ausführungsform des erfindungsgemäßen Verfahrens;

[0037] **Fig.** 2 eine schematische Darstellung der Teilnehmer und eines speziellen Systemaufbaus bei der ersten Ausführungsform des erfindungsgemäßen Verfahrens;

[0038] **Fig.** 3 das Grundprinzip der ersten Ausführungsform des erfindungsgemäßen Verfahrens;

[0039] **Fig.** 4 die Initialisierungsvorprozedur INI bei der ersten Ausführungsform der vorliegenden Erfindung;

[0040] **Fig.** 5 das Identitätsmodul auf der Seite des Mobiltelefons und dessen Funktion bei der ersten Ausführungsform der vorliegenden Erfindung;

[0041] **Fig.** 6 die Smard-Card auf der Seite des Prüfers und deren Funktion bei der ersten Ausführungsform der vorliegenden Erfindung;

[0042] **Fig.** 7 eine schematische Darstellung eines bekannten Identifikationsmechanismus eines Mobiltelefons gegenüber einem Netzwerkbetreiber; und

[0043] **Fig.** 8 eine schematische Darstellung eines weiteren bekannten Identifikationsmechanismus eines Mobiltelefons gegenüber einem Netzwerkbetreiber nach der Challenge & Response-Technik.

BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

[0044] In den Figuren bezeichnen gleiche Bezugszeichen gleiche oder funktionsgleiche Komponenten.

[0045] **Fig.** 1 zeigt eine schematische Darstellung der Teilnehmer und des allgemeinen Systemaufbaus bei einer ersten Ausführungsform des erfindungsgemäßen Verfahrens.

[0046] Die Identitäten für die Systemteilnehmer werden von vielen Identitätsgeneratoren (Identitätsinhaber) erzeugt. Die Anzahl der Identitätsgeneratoren nach **Fig.** 1 ist n (natürliche Zahl), also sind die Identitätsgeneratoren IG_1, IG_2 ... IG_n. G1, G2 bezeichnen verschiedene Gruppen für den Identitätsgenerator IG_1.

[0047] Die Anzahl der Identitätsprüfer ist m (natürliche Zahl), also sind die Identitätsprüfer IP_1 ... IP_m. OD in **Fig.** 1 bezeichnet ein offenes Verzeichnis mit SC1, ..., SCn als n feri verfügbaren Smart-Cards.

[0048] **Fig.** 2 zeigt eine schematische Darstellung der Teilnehmer und eines speziellen Systemaufbaus bei der ersten Ausführungsform des erfindungsgemäßen Verfahrens.

[0049] Hierbei handelt es sich um ein Mobiltelefonsystem mit n Mobiltelefon-Herstellern als Identitätsgeneratoren M_1

... M_n für individuelle Identifikationen IMEI1, IMEI2, etc. Im System sind m Identitätsprüfer als Dienstanbieter OP_1 ... OP_m. Hier wird darauf hingewiesen, dass die Identität nicht ausschließlich vom Hersteller generiert und geprüft werden kann, sondern auch von anderen Quellen Auth, wie eine Behörde oder weitere Systemadministratoren.

[0050] Jeder Dienstanbieter OP_1 ... OP_m und/oder Systemüberwacher oder Administrator soll in der Lage sein, ohne große Datenhaltung, die Identität eines Funktelefons, genannt IMEI (International Mobile Equipment Identity), auf Echtheit zu prüfen.

[0051] Echtheit bedeutet hier, dass diese Geräte tatsächlich vom Hersteller stammen, und dass der Hersteller die IMEI vergeben hat, was hier indirekt bedeutet, dass der Hersteller für die Qualität des Geräts und seine technischen Merkmale beim Verlassen der Fabrik haftet.

[0052] **Fig.** 3 zeigt das Grundprinzip der ersten Ausführungsform des erfindungsgemäßen Verfahrens.

[0053] Diese Ausführungsform erlaubt jedem Dienstanbieter OP_1 ... OP_m oder jeder Behörde oder Dritten die Echtheit der Identität für jedes Gerät M im Netz zu überprüfen, ohne das Mobiltelefon bzw. Gerät zu sehen. Der Prüfer P braucht ferner keine Abfrage bei dem Hersteller und braucht auch keine Liste von Serien- oder IMEI-Nummern und deren einzelnen Geheimschlüsseln. Der Prüfer P braucht lediglich eine elektronische Karte oder Smard-Card MSC vom Hersteller (oder vom Identitätsgeber/-inhaber), und braucht nur einmal ein offenes Verzeichnis OR des Herstellers (z. B. Internet) abzufragen. Jeder Hersteller bietet eine Smart-Card für jeden Prüfer P. Diese Smart-Cards MSC sind als ein Teil des offenen Verzeichnis OR zu betrachten, wie in **Fig.** 3 dargestellt ist.

[0054] Das Identifizierungsverfahren gemäß dieser Ausführungsform läuft prinzipiell folgendermaßen ab:
Der Identitätsgeber initialisiert das Mobiltelefon M in einer von einem Zertifizierungsbereich CC ausgeführten Vorprozedur INI, indem er es mit einer geheimen Identität SIMEI versieht, welche in einem beschreibbaren, aber nicht-lesbaren Speicher im Identifizierungsmodul **2'** des Geräts M abgelegt wird. Weiterhin erhält das Identifizierungsmodul **2'** die Fähigkeit, auf eine Anfrage hin eine vorbestimmte Identifizierungsprozedur abzuarbeiten. Dabei sollte das Identifizierungsmodul **2'** ein lebenswichtiger Bestandteil des Geräts M sein, was bedeutet, daß ein Entfernen bzw. Austauschen des Identifizierungsmoduls **2'** zu einem Funktionsverlust führt. Weiterhin erhält das Gerät M eine offen übertragbare Identität IMEI versieht, welche in einem nicht-flüchtigen, nach Erstbeschreibung nicht modifizierbaren Speicher des Geräts M abgelegt wird.

[0055] Der Prüfer P fordert die Identität des Mobiltelefons M durch eine Identitätsanfrage (Identity Request) IR, mit der zusammen ein Parameter CHv übermittelt wird.

[0056] Das Mobiltelefon M sendet darauf seine Identität IMEI zusammen mit einer elektronischen Unterschrift SIGt des Identitätsgebers (Herstellers) und einem weiteren Parameter CHt an den Prüfer P.

[0057] Der Prüfer P fragt einen Hersteller-Prüfschlüssel EMIGK vom offenen Verzeichnis OR im Internet ab.

[0058] Der Prüfer P überzeugt sich von der Unterschrift des Herstellers durch die Smart-Card MSC vom Hersteller und entscheidet, ob die Identität echt ist oder nicht. Dazu erzeugt er mittels der Parameter IMEI, CHv, CHt und EMIGK eine entsprechende elektronische Unterschrift SIGv und vergleicht diese mit der übermittelten elektronischen Unterschrift SIGt. Stimmen beide elektronischen Unterschriften SIGt und SIGv überein, ist die Identität echt, ansonsten nicht.

[0059] Im Detail werden die Systemvorgänge und Mechanismen nachstehend anhand von **Fig.** 4 bis 6 erläutert.

[0060] **Fig.** 4 zeigt die Initialisierungsvorprozedur INI bei der ersten Ausführungsform der vorliegenden Erfindung.

[0061] Der Hersteller/Identitätsgeber vergibt die Identität IMEI für sein Gerät M als Zusatz zur Seriennummer nach dem Verfahren, die im Standard vereinbart ist.

[0062] Der Hersteller schreibt im Gerät M in ein geschütztes Register die erste geheime Identität SIMEI, die der Hersteller durch eigenen geheimen Herstellerschlüssel MIGK (Master Identity Generator Key) erzeugt. Eine Einwegabbildung F1 generiert die erste geheime Identität SIMEI aus der Identität IMEI und dem Herstellerschlüssel MIGK:

$$SIMEI = F1 (IMEI, MIGK) \quad (1)$$

[0063] Jeder Hersteller kann für jede Gerätegruppe ein oder mehrere solcher MIGK Schlüssel vorsehen.

[0064] Der Hersteller veröffentlicht einen öffentlichen Schlüssel EMIGK in seiner offenen Internet-Homepage OMHP. EMIGK ist ein chiffriertes Abbild vom Herstellerschlüssel MIGK durch die Funktion F2 wobei:

$$EMIGK = F2 (MIGK, SMMK) \quad (2)$$

[0065] Dabei ist SMMK (Secret Manufacturer Master-Key) der Hauptgeheimschlüssel des Herstellers. Für jeden Gerättyp kann der Hersteller einen solchen Eintrag vorsehen oder einen Einzeleintrag für alle Hersteller Typen verwenden.

[0066] Der Hersteller hält die beiden Schlüssel SMMK und MIGK geheim. Allerdings liefert der Hersteller die Smart-Card MSC an den oder die Prüfer P, welche SMMK in einem geschützten und nicht lesbaren Register enthält (vgl. **Fig.** 6) und die inverse Funktion zu F2, also $F2^{-1}$, enthält, die aus SMMK und EMIGK den Herstellerschlüssel MIGK erzeugen kann.

[0067] Alle Zwischenergebnisse in der Smart-Card MSC (**Fig.** 6) und im Identifizierungsmodul **2'** (**Fig.** 5) sind physikalisch nicht erreichbar (d. h. weder zum Schreiben noch zum Lesen). Dies sollte bei der Herstellung gewährleistet werden.

[0068] Der Hersteller kann zur Sicherheit die Smart-Card MSC selbst herstellen, um die o. g. Bedingungen zu erfüllen, oder diese von einem vertrauenswürdigen Dritten beziehen.

[0069] **Fig.** 5 zeigt das Identitätsmodul auf der Seite des Mobiltelefons und dessen Funktion bei der ersten Ausführungsform der vorliegenden Erfindung.

[0070] Der Prüfer P, z. B. der Netzoperator oder die Behörde, fragt das Gerät M nach seiner Identität und der Anfrage IR und fordert eine Signatur für den mitgelieferten Zufallswert CHv.

[0071] Das Gerät M generiert in seinem Identitätsmodul **2'** die elektronische Unterschrift SIGt als Funktion der ersten geheimen Identität SIMEI und CHv und eines neuen Zufallswerts CHt, der durch das Gerät M generiert wird, mittels der Krypto-Funktion F3:

$$SIGt = F3 (SIMEI, CHv, CHt) \quad (3)$$

[0072] Die elektronische Unterschrift SIGt wird zusammen mit CHt und IMEI an den Prüfer P als beglaubigte Identität gesendet, wie in **Fig.** 3 dargestellt ist. CHv liegt bereits beim Prüfer P vor, da es dort generiert wurde.

[0073] Der Prüfer P berechnet die entsprechende elektronische Unterschrift SIGv aus IMEI, CHt, CHv durch die gleiche Krypto-Funktion F3:

SIGv = F3 (IMEI, CHv, CHt) (4)

[0074] Falls SIGt = SIGv, dann wird IMEI als authentisch betrachtet.

[0075] Im Gerät M ist ein geschützter Bereich eingerichtet, der ein nicht-lesbares Register mit SIMEI und der Krypto-Abbildung F3 sowie ein Register mit IMEI, das vorzugsweise nicht modifizierbar ist, enthält. Dazu enthält das Gerät M einen Zufallsgenerator CHt. Alle diese Einheiten werden in einer geschützten physikalischen Einheit, hier im Identitätsmodul 2', zusammen integriert, wie in **Fig.** 5 dargestellt. Zur Erzeugung der elektronischen Unterschrift SIGt des Geräts M werden folgende Schritte getätigt:
Ein Zufallswert CHt wird neu generiert.

[0076] CHv und CHt werden zusammen mit SIMEI durch die Krypto-Einweg-Funktion F3 verknüpft. Z. B. kann CHt XOR CHv erst erzeugt und dann durch F3 mit SIMEI als Schlüssel abgebildet werden, wie in **Fig.** 5 gezeigt ist. Es ist ebenfalls möglich, wie in **Fig.** 5 gezeigt, CHv und CHt zu multiplexen (Multiplexer-Steuerung nicht gezeigt) und dann dem XOR (+) zuzuführen, wobei es eine Rückkopplung vom Ausgang von F3 zum XOR (+) gibt.

[0077] Das Gerät M liefert dann als prüfbaren Identitätsvektor das folgende Prüfvektor-Tupel an den Prüfer:

Prüfvektor = (IMEI, SIGt, CHt, CHv)

[0078] Durch die Identität IMEI, die als offene Identität gilt, werden der Gerätetyp und -hersteller bekannt. Der Prüfer P kann dann leicht von den offenen Verzeichnis OR des Herstellers den dazugehörigen offenen Prüfschüssel EMIGK vom Internet abholen. Alternativ könnte der Prüfer eine Liste vom Hersteller verwalten und von Zeit zu Zeit aktualisieren, um im Internet Zugriffe zu sparen, und nur zum Internetverzeichnis der Hersteller gehen, falls der Hersteller neue Typen bietet.

[0079] **Fig.** 6 zeigt die Smard-Card auf der Seite des Prüfers und deren Funktion bei der ersten Ausführungsform der vorliegenden Erfindung.

[0080] Der Prüfer P empfängt vom Mobiltelefon M den Prüfvektor und überprüft, ob die Signatur SIGt die Identität des Geräts nachweist, also SIGv = SIGt gilt. Der Prüfer P hat danach den Beweis, daß die vom Gerät M behauptete IMEI tatsächlich vom Hersteller stammt. Für diesen Zweck ist die Smart-Card MSC vom Hersteller notwendig, die verfügbar für jeden Prüfer P sein soll. Diese Smart-Card MSC nach **Fig.** 6 enthält alle drei Abbildungen F1, $F2^{-1}$ und F3 sowie ein geschütztes einmal beschreibbares Register mit dem geheimen Schlüssel SMMK, als Hersteller/Identitätsgeber Master Geheimschlüssel (Secret Manufacturer Master Key). SMMK wird, wie gesagt, durch Hersteller/Identitätsträger in die Smart-Card MSC eingeschrieben. SMMK ist physikalisch nicht lesbar. Die geschützten Schlüssel im übrigen folgende Regeln erfüllen:

1. Sie sind physikalisch nicht lesbar, und zwar vorzugsweise auch bei destruktivem Öffnen der Vorrichtung.
2. Sie sind nur überschreibbar, wenn der Schreiber den aktuellen Inhalt kennt.

[0081] Der Prüfer P führt den Prüfvektor der Smart-Card MSC zu und führt folgende Operationen durch:

[0082] Der Prüfer P holt vom Internet den Hersteller-Prüfschlüssel EMIGK, nachdem er IMEI bzw. Type des Geräts und Name des Herstellers vom Gerät M erhält.

[0083] Der Prüfer P gibt die empfangenen Komponenten des Prüfvektors zusammen mit EMIGK in die Smart-Card MSC ein. Die Smart-Card MSC dechiffriert erst EMIGK mit Hilfe des Schlüssels SMMK und der dechiffrierten Funktion $F2^{-1}$. Daraus ergibt sich der Hersteller/Identitätsgeber Master Geheimschlüssel MIGK. Die Hard- und Software der Smart-Card MSC dürfen dabei das Lesen von MIGK nicht ermöglichen.

[0084] Die erste geheime Identität SIMEI wird dann generiert. Dies geschieht durch Verwendung von MIGK und IMEI über die Funktion F1, wie **Fig.** 6 zeigt. Die Hard- und Software der Smart-Card MSC dürfen wiederum das Lesen von SIMEI nicht ermöglichen.

[0085] SIMEI wird intern mit den beiden Zufallsgrößen CHt, CHv über die Funktion F3 in gleicher Art und Weise wie in der Smart-Card MSC verknüpft, um die elektronische Unterschrift SIGv zu bekommen.

[0086] Falls SIGv = SIGt, dann gilt die Identität IMEI als echt, und die Identität des Geräts ist akzeptiert, ansonsten ist die Identifizierung gescheitert.

[0087] Obwohl die vorliegende Erfindung vorstehend anhand eines bevorzugten Ausführungsbeispiels beschrieben wurde, ist sie darauf nicht beschränkt, sondern auf vielfältige Weise modifizierbar.

[0088] Für die Abbildungen F1, F2 und F3 kann die standardisierte Kryptofunktion im Mobiltelefonsystem verwendet werden. In diesem Fall wird F1 = F2 = F3 = SF (Standard-Funktion) angenommen.

[0089] Das vereinfacht den Aufbau der Smart-Card MSC, da solche Smart-Cards ohnehin im System existieren, können die Hersteller solche verwenden. Da auch SF im Mobiltelefon vorhanden ist, resultiert daraus eine im Endeffekt sehr effektive Implementierung.

Patentansprüche

1. Verfahren zur Identifikation einer physikalischen Einheit (M) in einem offenen, drahtlosen Telekommunikationsnetzwerk durch eine Prüfeinrichtung (P) mit den Schritten:
   a) Speichern einer geheimen Identität (SIMEI) und einer offenen Identität (IMEI) in der physikalischen Einheit (M);
   b) Erzeugen eines ersten Parameters (CHv) in der Prüfeinrichtung (P)
   c) Senden einer Identifikationsaufforderung (IR) mit dem ersten Parameter (CHv) von der Prüfeinrichtung (P) an die physikalische Einheit (M);
   d) Erzeugen einer elektronischen Unterschrift (SIGt) durch eine erste Krypto-Funktion (F3) aus der geheimen Identität (SIMEI) und mindestens dem ersten Parameter (CHv) in der physikalischen Einheit (M) und Senden der erzeugten elektronischen Unterschrift (SIGt) und der offenen Identität (IMEI) an die Prüfeinrichtung (P);
   e) Erzeugen der geheimen Identität (SIMEI) aus einem offenen Schlüssel (EMIGK) und der gesendeten offenen Identität (IMEI) in der Prüfeinrichtung (P);
   f) Erzeugen einer entsprechenden elektronischen Unterschrift (SIGv) durch die erste Krypto-Funktion (F3) aus der erzeugten ersten geheimen Identität (SIMEI) und mindestens dem ersten Parameter (CHv) in der Prüfeinrichtung (P); und
   g) Identifizieren der physikalischen Einheit (M) durch einen Vergleich der gesendeten elektronischen Unterschrift (SIGt) und der erzeugten entsprechenden elektronischen Unterschrift (SIGv) in der Prüfeinrichtung (P).
2. Verfahren nach Anspruch 1, dadurch gekennzeich-

net, daß der offene Schlüssel (EMIGK) durch eine zweite Krypto-Funktion (F2) aus einem ersten geheimen Schlüssel (SMMK) und einem zweiten geheimen Schlüssel (MIGK) erzeugt wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die geheime Identität (SIMEI) durch eine dritte Krypto-Funktion (F1) aus der offenen Identität (IMEI) und dem zweiten geheimen Schlüssel (MIGK) erzeugt wird.

4. Verfahren nach Anspruch 3, in Verbindung mit Anspruch 2, dadurch gekennzeichnet, daß in der Prüfeinrichtung (P) der erste geheime Schlüssel (SMMK) gespeichert wird und die geheime Identität (SIMEI) durch folgende Schritte in der Prüfeinrichtung (P) erzeugt wird:

Erzeugen des zweiten geheimen Schlüssels (MIGK) durch die Inverse ($F2^{-1}$) zur zweiten Krypto-Funktion (F2) aus dem ersten geheimen Schlüssel (SMMK) und dem offenen Schlüssel (EMIGK); und

Erzeugen der geheimen Identität (SIMEI) durch die dritte Krypto-Funktion (F1) aus aus der offenen Identität (IMEI) und dem erzeugten zweiten geheimen Schlüssel (MIGK).

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der offene Schlüssel (EMIGK) über das Internet an die Prüfeinrichtung gesendet wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch die Schritte:

Erzeugen eines zweiten Parameters (CHt) in der physikalischen Einheit (M);

Senden des zweiten Parameters (CHt) an die Prüfeinrichtung (P); und

Erzeugen der elektronischen Unterschrift (SIGt) und der entsprechenden elektronischen Unterschrift (SIGv) aus der geheimen Identität (SIMEI) und dem ersten und zweiten Parameter (CHv; CHt).

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß der erste und der zweite Parameter (CHv; CHt) durch eine exklusive ODER-Funktion (+) verknüpft werden.

8. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß der erste und der zweite Parameter (CHv; CHt) multiplexiert und anschließend durch eine exklusive ODER-Funktion (+) verknüpft werden, wobei es eine Rückkopplung vom Ausgang der ersten Krypto-Funktion (F3) zur exklusiven ODER-Funktion (+) gibt.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der erste und/oder zweite Parameter (CHv; CHt) als Zufallsgrößen vorgesehen werden.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Telekommunikationsnetzwerk ein Mobiltelefonsystem ist.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die erste, zweite und dritte Krypto-Funktion (F1; F2; F3) die gleiche Funktion sind.

12. Verfahren nach Anspruch 11, in Verbindung mit Anspruch 9, dadurch gekennzeichnet, daß die gleiche Funktion eine Standardfunktion ist.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Schritte d) und e) auf einer Smard-Card (MSC) in der Prüfeinrichtung (P) durchgeführt werden.

Hierzu 4 Seite(n) Zeichnungen

Nummer: DE 100 26 326 A1
Int. Cl.[7]: H 04 Q 7/34
Offenlegungstag: 29. November 2001

FIG 1

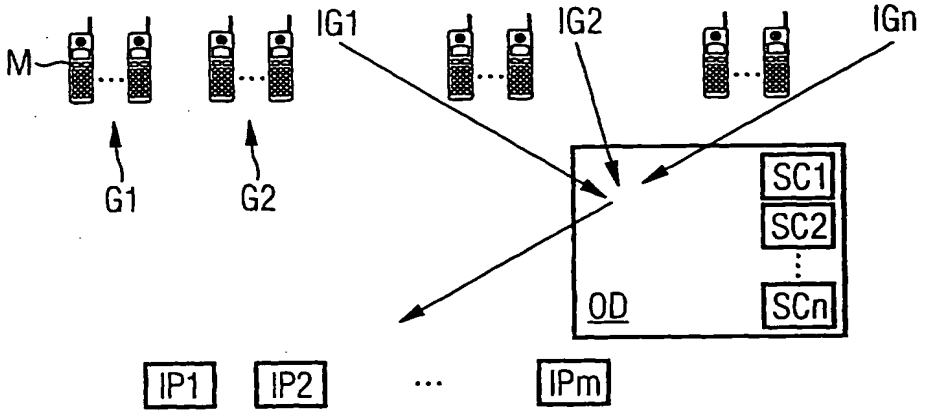
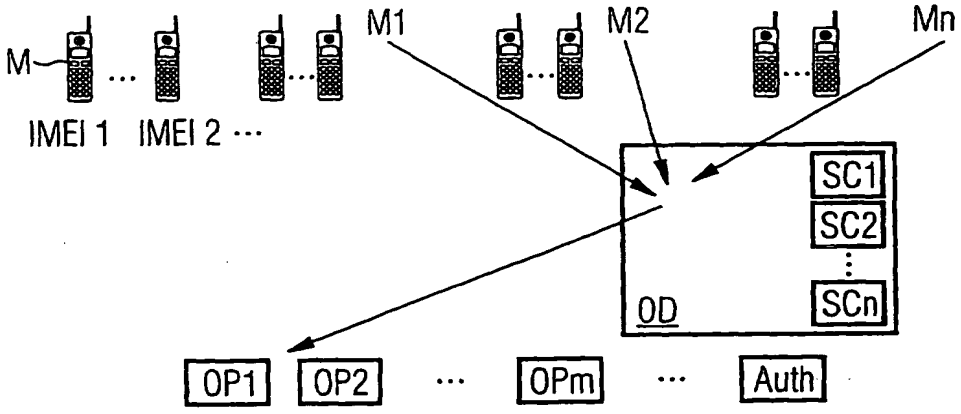


FIG 2



Nummer: DE 100 26 326 A1
Int. Cl.[7]: H 04 Q 7/34
Offenlegungstag: 29. November 2001

FIG 3

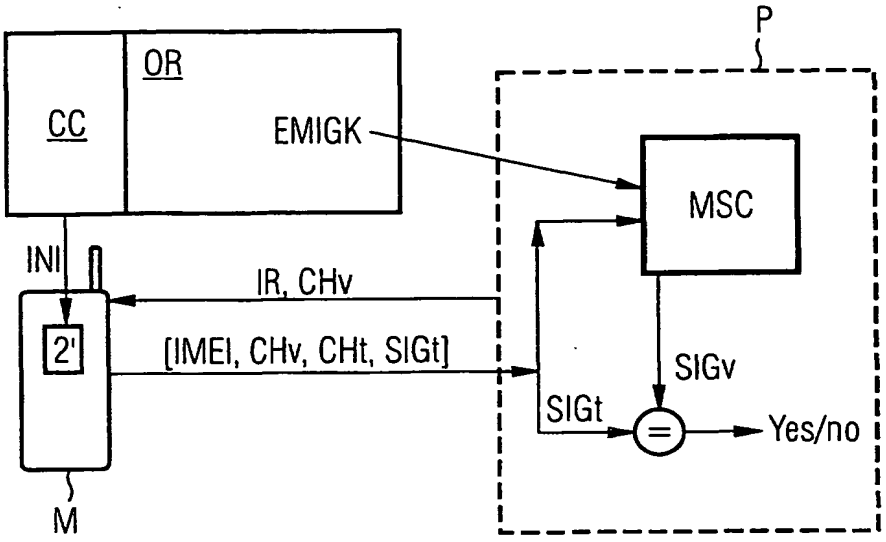
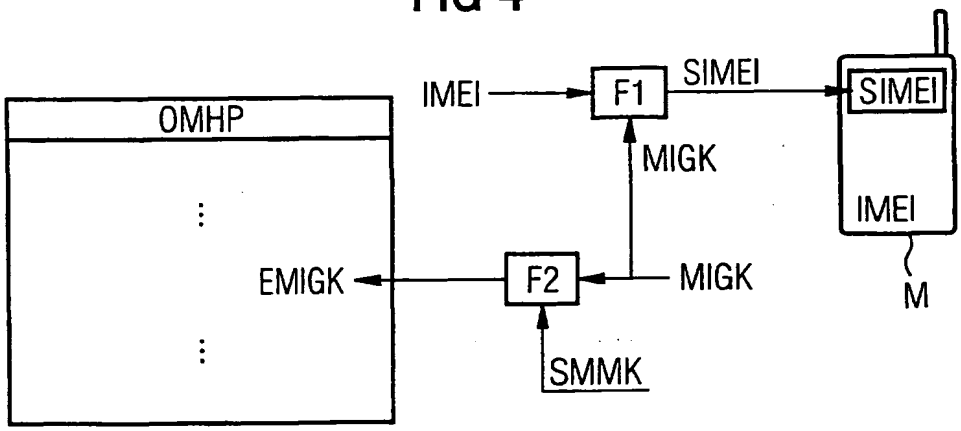


FIG 4



Nummer: DE 100 26 326 A1
Int. Cl.[7]: H 04 Q 7/34
Offenlegungstag: 29. November 2001

FIG 5

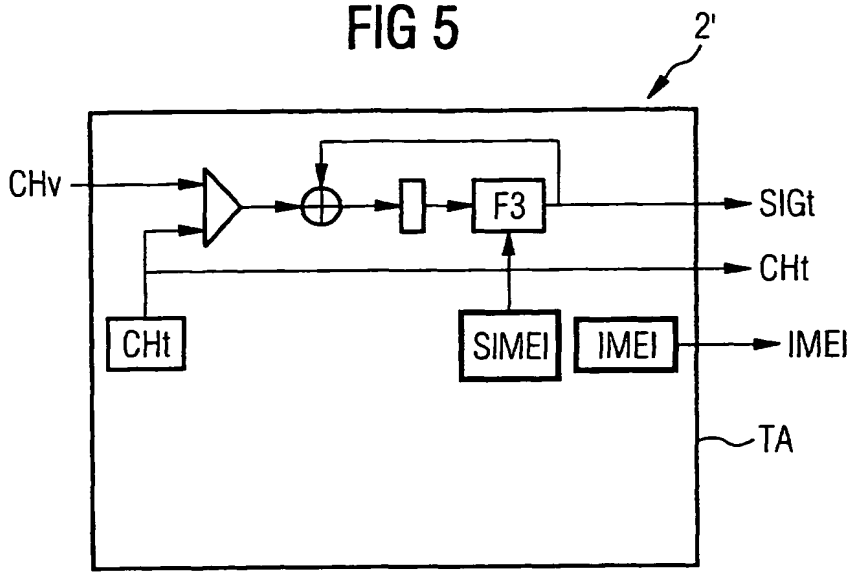
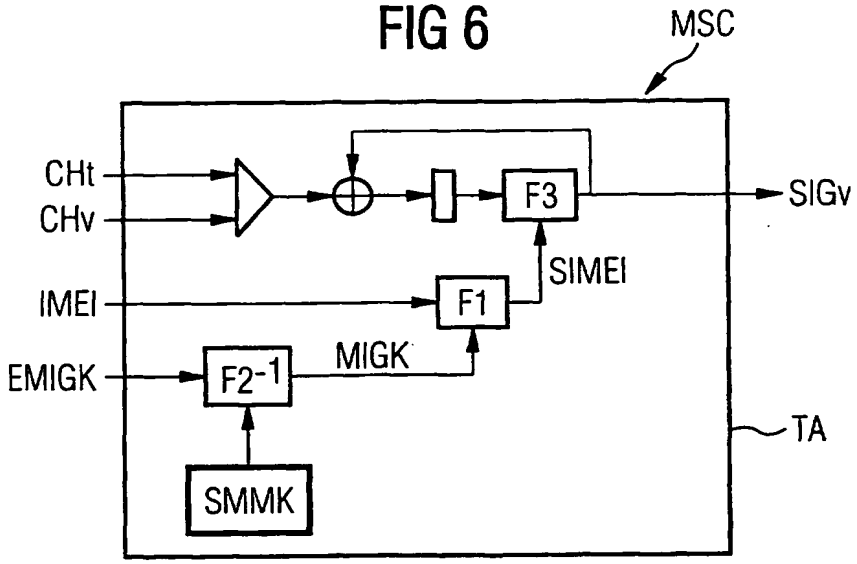


FIG 6



Nummer: DE 100 26 326 A1
Int. Cl.[7]: H 04 Q 7/34
Offenlegungstag: 29. November 2001

FIG 7

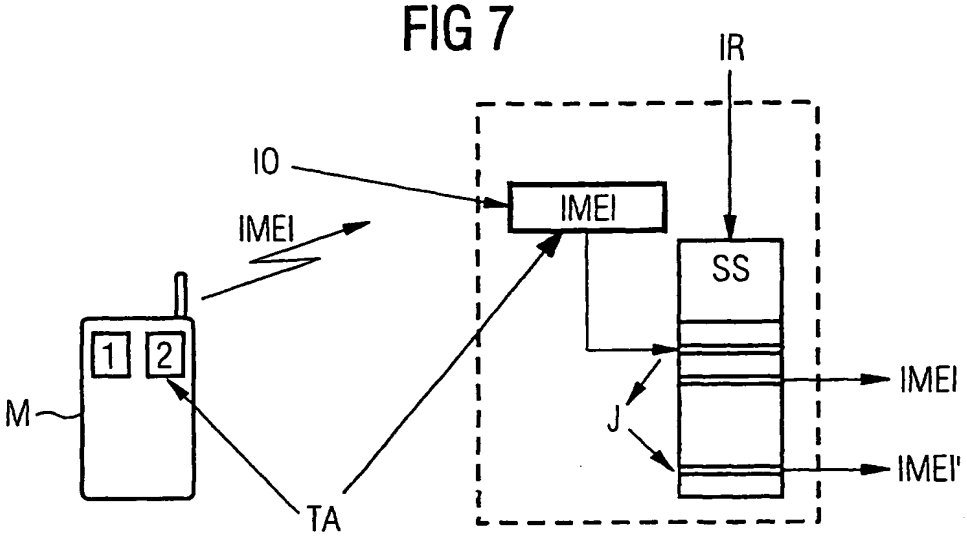


FIG 8